UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,439	03/02/2004	Ori Eisen	2311.008	3435

7590 12/07/2007

U.P. PETER ENG
WILSON SONSINI GOODRICH AND ROSATI
650 PAGE MILL ROAD
PALO ALTO, CA 94304

EXAMINER	
ZELASKIEWICZ, CHRYSTINA E	
ART UNIT	PAPER NUMBER
4143	

MAIL DATE	DELIVERY MODE
12/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,439	EISEN, ORI	
	Examiner	Art Unit	
	Chrystina Zelaskiewicz	4143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :11/5/2007, 2/6/2007, 12/1/2006, 3/24/2006, 10/21/2005.

DETAILED ACTION

Status of Claims

1. This action is in reply to the application filed on 2 March 2004.

2. Claims 1-18 are currently pending and have been examined.

Information Disclosure Statement

3. The Information Disclosure Statements filed on 5 November 2007, 6 February 2007, 1 December 2006, 24 March 2006, and 21 October 2005 have been considered. Initialed copies of the Form 1449 are enclosed herewith.

Drawings

4. The subject matter of this application admits of illustration by a drawing to facilitate understanding of the invention. Applicant is required to furnish a drawing of at least the method flowcharts under 37 CFR 1.81(c). No new matter may be introduced in the required drawing. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

5. Claims 1-11 in the current application are directed to a process. Therefore, flowcharts would facilitate an understanding of the invention. See 37 CFR 1.81(b).

Specification

6. The disclosure is objected to because of the following informalities: page 5 of the specification refers to "the chart," but there is no corresponding "chart" filed in the original disclosure. Furthermore, the specification has no figure or reference numbers that correspond to "the chart." Examiner notes the following items regarding the chart: a petition to expunge was filed on 25 August 2005; and a preliminary amendment was filed on 14 February 2006.

Appropriate correction is required.

7. The use of the trademark MICROSOFT ® has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner that might adversely affect their validity as trademarks.

Claim Objections

8. Claim 17 is directed to a medium because it has the limitation *a computer readable medium as claims in claim 11*. However, claim 11 is directed to a method. For purposes of this examination, the examiner will assume that the applicant meant *a computer readable medium* ***as in claim 12***.

Claim Rejections - 35 USC § 112, 2nd paragraph

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1 and 12 and their respective dependent claims 2-11, 18 and 13-17 are rejected under 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. With respect to claim 1, the limitation *uniquely identifying said customer with said delta of time parameter and said at least one personal or non-personal identification parameter* is vague and indefinite because applicant does not specify how to **uniquely** identify said customer with the other two parameters. For purposes of this examination, the examiner will assume that the applicant meant *identifying said customer with said delta of time parameter and said at least one personal or non-personal identification parameter*.

12. With respect to claim 12, the limitation *uniquely identifying said customer with customer identification customer identification data comprising said delta of time parameter and said at least one of either of said personal or non-personal identification parameter* is vague and indefinite. For purposes of this examination, the examiner will assume that the applicant meant *identifying said customer with* ***customer identification*** *data comprising said delta of time parameter and* ***at least one of either said personal or said non-personal identification parameter***.

13. Claim 1 recites the following limitations: *said customer's computer* in line 3; *the clock* in line 5; *said server's local time* in line 7; and *said customer* in line 10. There is insufficient antecedent basis for these limitations in the claim.

14. Claim 3 recites the limitation *said computer's IP address* in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

15. Claim 4 recites the limitation *said computer's Browser ID* in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

16. Claim 7 recites the limitation *the website operator* in line 2. There is insufficient antecedent basis for this limitation in the claim.

17. Claim 12 recites the following limitations: *the clock of said customer's computer* in line 5; *said computer's local time* in line 5; *the clock of said website's server computer* in line 6; *said server computer's local time* in lines 6-7; and *said customer* in line 10. There is insufficient antecedent basis for these limitations in the claim.

18. Claim 14 recites the limitation *the website operator* in line 2. There is insufficient antecedent basis for this limitation in the claim.

19. Claims 14-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The limitation *indication as to whether a second online transaction **may** be fraudulent* is vague and indefinite because applicant does not affirmatively state whether or not the online transaction is fraudulent. For purposes of this examination, the examiner will assume that the applicant meant *indication as to whether a second online transaction **is or is not** fraudulent*.

Claim Rejections - 35 USC § 101

20. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

21. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in **most**

cases since use of technology permits the function of the descriptive material to be realized. See MPEP § 2106.01.

22. Claims 12-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 12-18 are directed to *a computer readable medium containing program instructions*. However, claims 12-18, as currently written, do not have the functional descriptive material (program instructions) as structurally and functionally interrelated to the medium. Instead, claims 12-18 should be directed to **executable** program instructions that are **tangibly embodied** on a computer readable medium.

Claim Rejections - 35 USC § 102

23. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Examiner's Note: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

24. Claims 1, 5 and 12 are rejected under 35 U.S.C. 102(e) as being anticipated by Shinzaki (US 6,957,339 B2).

Claim 1

Shinzaki, as shown, discloses the following limitations:

- *receiving, from said customer's computer, at least one personal or non-personal identification parameter* (see at least column 3, lines 66-67 and column 4, lines 1-9: The portable electronic device includes: a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of the portable electronic device; a second transceiving interface for transmitting/receiving data to/from the data processing device; a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from an external device via the second transceiving interface, with the valid biometric feature data; and a PIN register section having a pre-stored PIN of the authorized user of the portable electronic device);
- *capturing, from the clock of said customer's computer, said customer's computer local time* (see at least column 4, lines 57-58: a time stamp generating section for generating a time stamp as the date and time);
- *capturing, from a website's server clock, said server's local time* (see at least column 4, lines 65-66: a clock function section for calculating the current time);
- *creating and storing a delta of time parameter based upon the difference between said customer's computer local time and said server's local time* (see at least column 4, lines 66-67 and column 5, lines 1-3: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section);
- *uniquely identifying said customer with said delta of time parameter and said at least one personal or non-personal identification parameter* (see at least column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section).

Claim 5

Shinzaki discloses the limitations of claim 1 as shown above. Furthermore, Shinzaki, as shown, discloses the following limitation:

- *said delta of time parameter is stored as a range of time* (see at least column 4, lines 66-67 and column 5, lines 1-3, 8-10: a time stamp verifying section for comparing the original time

stamp… with the current time, which has been calculated by the clock function section… difference between the time stamp and the current time falls within a predetermined range).

Claim 12

Shinzaki, as shown, discloses the following limitations:

- *receiving, from an online customer' s computer, at least one of either a personal or non-personal identification parameter* (see at least column 3, lines 66-67 and column 4, lines 1-9: The portable electronic device includes: a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of the portable electronic device; a second transceiving interface for transmitting/receiving data to/from the data processing device; a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from an external device via the second transceiving interface, with the valid biometric feature data; and a PIN register section having a pre-stored PIN of the authorized user of the portable electronic device);
- *capturing, from the clock of said customer's computer, said computer's local time* (see at least column 4, lines 57-58: a time stamp generating section for generating a time stamp as the date and time)*;*
- *capturing, from the clock of said website's server computer, said server computer's local time* (see at least column 4, lines 65-66: a clock function section for calculating the current time);
- *creating and storing a delta of time parameter based upon the difference between said customer's computer's local time and said server computer's local time* (see at least column 4, lines 66-67 and column 5, lines 1-3: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section); and
- *uniquely identifying said customer with customer identification customer identification data comprising said delta of time parameter and said at least one of either of said personal or non-personal identification parameter* (see at least column 5, lines 12-15: the user is

identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section).

Claim Rejections - 35 USC § 103

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

26. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

27. Claims 2-3, 6-10, 13-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinzaki in view of Ronning et. al. (US 7,165,051 B2).

Claim 2

Shinzaki discloses the limitations of claim 1 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *receiving, from said customer, an additional identification parameter comprising personal identification information relating to said transaction* (see at least column 7, lines 55-59: Order form 520 includes a number of sections for receiving the following information for use in submitting an order: name section 521; company name section 522; address section 523; phone section 524; e-mail address section 525; credit card number section 526; and password section 527).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning

because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning).

Claim 3

Shinzaki discloses the limitations of claim 1 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *said at least one non-personal identification parameter is said computer's IP address* (see at least column 8, lines 22-23: information may include the following for each order… IP address).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning).

Claim 6

Ronning, as shown, discloses the following limitations:

- *creating a first computer identifier in the course of an online transaction comprising the steps of Claim 1* (Shinzaki discloses the limitations of claim 1 as shown above);
- *creating at least a second computer identifier in the course of a second proposed online transaction comprising the steps of Claim 1* (Shinzaki discloses the limitations of claim 1 as shown above);
- *utilizing a matching parameter to compare said first computer identifier with said second computer identifier* (see at least column 9, lines 48-59: The fraud processing involves generating a fraud ranking based upon the user's information in order form 520 and associated information. The associated information may include any information, or a sub-set of that information, having any type of relation to the information submitted with the order. For example, it typically includes information linked with the submitted information as determined by the relational database tables illustrated in FIG. 5C. It may also include a previous fraud

ranking or an AVS rating. System 200 may use the submitted information to perform database look ups to obtain associated information for analysis);

- *creating a matching value based on the similarities between said first computer identifier and said second computer identifier* (see at least column 9, lines 65-67 and column 10, line 1: The fraud processing involves comparing the fraud ranking to a particular fraud scale (step 505); for example, a numeric scale with increasing numbers indicating an increasing likelihood of a fraudulent transaction); and
- *classifying said second online transaction as fraudulent, not fraudulent, or requiring further consideration based upon the value of said matching parameter* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 7

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *communicating to the website operator an indication, as to whether said second online transaction is fraudulent, not fraudulent, or requires further consideration* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a

likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 8

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *blocking said second online transaction based upon the value of said matching parameter* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 9

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *communicating to said customer the status of said second online transaction based upon the value of said matching parameter* (see at least column 7, lines 39-42: System 200 determines if the user is attempting a fraudulent transaction and, if not, it downloads the purchased products to the user's machine using a download page 516; also see at least column 9, lines 34-37: If authorization is not obtained (step 503), system 200 declines the order (step 509) and typically presents a message to the user indicating the denial).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 10

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Shinzaki, as shown, discloses the following limitation:

- *said delta of time parameter is stated as a range of time* (see at least column 4, lines 66-67 and column 5, lines 1-3, 8-10: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section… difference between the time stamp and the current time falls within a predetermined range).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are

distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 13

Shinzaki discloses the limitations of claim 12 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *receiving and storing, from said customer, personal identification information relating to said transaction* (see at least figure 2 as well as column 3, lines 65-67 and column 4, line 1: A log in module 208 receives the request and records certain data associated with the request, such as the user's request, Internet Protocol (TIP) address, date and time, and particular demographic information).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning).

Claim 14

Shinzaki discloses the limitations of claim 12 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *communicating to the website operator an indication as to whether a second online transaction may be fraudulent because of the similarity existing between the stored customer identification data and the new customer's identification data* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria; also see at least column 12, lines 8-11: system 200 compares particular main information on the same order against known profiles indicating attempted fraudulent

transactions (step 712), and it determines if the main information matches the known profiles).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning).

Claim 15

Shinzaki, in view of Ronning, discloses the limitations of claim 14 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *blocking said second online transaction based upon said indication as to whether a second online transaction may be fraudulent* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning).

Claim 16

Shinzaki, in view of Ronning, discloses the limitations of claim 14 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *communicating to said customer the status of said second online transaction based upon the similarity of said stored customer identification data and the new customer's identification data* (see at least column 7, lines 39-42: System 200 determines if the user is attempting a fraudulent transaction and, if not, it downloads the purchased products to the user's machine using a download page 516; also see at least column 9, lines 34-37: If authorization is not obtained (step 503), system 200 declines the order (step 509) and typically presents a message to the user indicating the denial).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning).

Claim 18

Ronning, as shown, discloses the following limitations:

- *creating a first computer identifier in the course of an online transaction comprising the steps of Claim 1* (Shinzaki discloses the limitations of claim 1 as shown above);
- *creating at least one additional computer identifier in the course of an additional online transaction comprising the steps of Claim 1* (Shinzaki discloses the limitations of claim 1 as shown above);
- *utilizing a matching routine to compare said first computer identifier with said at least one additional computer identifier* (see at least column 9, lines 48-59: The fraud processing involves generating a fraud ranking based upon the user's information in order form 520 and associated information. The associated information may include any information, or a sub-set of that information, having any type of relation to the information submitted with the order. For example, it typically includes information linked with the submitted information as determined by the relational database tables illustrated in FIG. 5C. It may also include a previous fraud ranking or an AVS rating. System 200 may use the submitted information to perform database look ups to obtain associated information for analysis); and
- *deciding as to whether the online transaction is fraudulent, not fraudulent or requires further consideration based on the similarities between said first computer identifier and said at least one additional computer identifier* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria; also

see at least column 12, lines 8-11: system 200 compares particular main information on the same order against known profiles indicating attempted fraudulent transactions (step 712), and it determines if the main information matches the known profiles).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

28. Claims 4 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinzaki in view of Boesch et. al. (US 6,092,053).

Claim 4

Shinzaki discloses the limitations of claim 1 as shown above. Furthermore, Boesch, as shown, discloses the following limitation:

- *said at least one non-personal identification parameter is said computer's Browser ID* (see at least column 7, lines 15-19: The message sent from the consumer's browser to the CIS (consumer information server) indicates whether the browser contains a browser identifier. In the preferred embodiment, the browser identifier is a cookie. A browser identifier identifies the consumer browser on a specific consumer computer).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the browser ID parameter of Boesch. As shown above, Shinzaki teaches capturing of certain parameters in order to validate a user to prevent fraud. Shinzaki fails to teach that one of the parameters captured is a computer's browser ID. However, Boesch teaches that capturing a browser ID was a well known parameter in order to detect fraud. Thus, it would have been obvious to combine Shinzaki with Boesch because a browser ID is a parameter that can be used to validate a user to prevent fraud.

Claim 17

Shinzaki discloses the limitations of claim 12 as shown above. Furthermore, Boesch, as shown, discloses the following limitation:

- *said non-personal computer identification parameter is a Browser ID* (see at least column 7, lines 15-19: The message sent from the consumer's browser to the CIS (consumer information server) indicates whether the browser contains a browser identifier. In the preferred embodiment, the browser identifier is a cookie. A browser identifier identifies the consumer browser on a specific consumer computer).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the browser ID parameter of Boesch. As shown above, Shinzaki teaches capturing of certain parameters in order to validate a user to prevent fraud. Shinzaki fails to teach that one of the parameters captured is a computer's browser ID. However, Boesch teaches that capturing a browser ID was a well known parameter in order to detect fraud. Thus, it would have been obvious to combine Shinzaki with Boesch because a browser ID is a parameter that can be used to validate a user to prevent fraud.

29. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shinzaki in view of Ronning, and further in view of Boesch.

Claim 11

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Boesch, as shown, discloses the following limitation:

- *said personal or non-personal identification parameter is a Browser ID* (see at least column 7, lines 15-19: The message sent from the consumer's browser to the CIS (consumer information server) indicates whether the browser contains a browser identifier. In the preferred embodiment, the browser identifier is a cookie. A browser identifier identifies the consumer browser on a specific consumer computer).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki, in view of the method of detecting fraud of

Ronning, with the browser ID parameter of Boesch. As shown above, Shinzaki teaches capturing of certain parameters in order to validate a user to prevent fraud. Ronning teaches the need for secure electronic commerce to prevent fraud. Both Shinzaki and Ronning fail to teach capturing a computer's browser ID to prevent fraud. However, Boesch teaches that capturing a browser ID was a well known parameter in order to detect fraud. Thus, it would have been obvious to combine Shinzaki, in view of Ronning, with Boesch because a browser ID is a parameter that can be used to prevent fraud.

Conclusion

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Chrystina Zelaskiewicz** whose telephone number is **571.270.3940.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James A. Reagan** can be reached at **571.272.6710**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov >. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**. Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

/Chrystina Zelaskiewicz/Examiner, Art Unit 4143
December 5, 2007
/James A. Reagan/Supervisory Patent Examiner, Art Unit 3621